Risoluzione dei problemi relativi a STP e considerazioni correlate sulla progettazione

Sommario

Introduzione

In questo documento vengono forniti suggerimenti per implementare una rete sicura su come collegare gli switch Cisco Catalyst con software Catalyst OS/Cisco IOS®.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento vengono descritti alcuni motivi di errore comuni del protocollo Spanning Tree Protocol (STP) e le informazioni da cercare per individuare la causa del problema. Mostra inoltre il tipo di struttura che riduce al minimo i problemi relativi allo spanning tree ed è facile da risolvere.

Questo documento non illustra le operazioni di base dell'STP. Per informazioni sul funzionamento dell'STP, consultare questo documento:

- Descrizione e configurazione dell'STP (Spanning Tree Protocol) sui Catalyst Switch

Questo documento non illustra il protocollo RSTP (Rapid STP), definito in IEEE 802.1w. Inoltre, questo documento non illustra il protocollo MST (Multiple Spanning Tree), definito in IEEE 802.1s. Per ulteriori informazioni sui protocolli RSTP e MST, consultare questi documenti:

- Informazioni sul protocollo Multiple Spanning Tree (802.1s)
- Informazioni sul protocollo Rapid Spanning Tree (802.1w)

Per informazioni più specifiche sulla risoluzione dei problemi dell'STP per i Catalyst switch che eseguono il software Cisco IOS, consultare il documento Risoluzione dei problemi dell'STP sui Catalyst switch che eseguono Cisco IOS integrato (modalità nativa).

Errore dello Spanning Tree Protocol

La funzione primaria dell'algoritmo STA (Spanning Tree Algorithm) è quella di eliminare i loop creati dai collegamenti ridondanti nelle reti bridge. L'STP opera al livello 2 del modello OSI (Open System Interconnection). Tramite unità dati di protocollo bridge (BPDU) scambiate tra bridge, l'STP elegge le porte che inoltrano o bloccano il traffico. Questo protocollo può fallire in alcuni casi specifici e risolvere la situazione che può risultare molto difficile, che dipende dalla progettazione della rete. In questa particolare area, è necessario eseguire la parte più importante del processo di risoluzione dei problemi prima che si verifichi il problema.

Un errore a livello di STA generalmente determina un bridging loop. La maggior parte dei clienti che chiamano il supporto tecnico Cisco per problemi di spanning tree sospetta un bug, ma raramente questa è la causa. Anche se il problema è il software, un loop di bridging in un ambiente STP continua a provenire da una porta che può bloccare, ma inoltra il traffico.

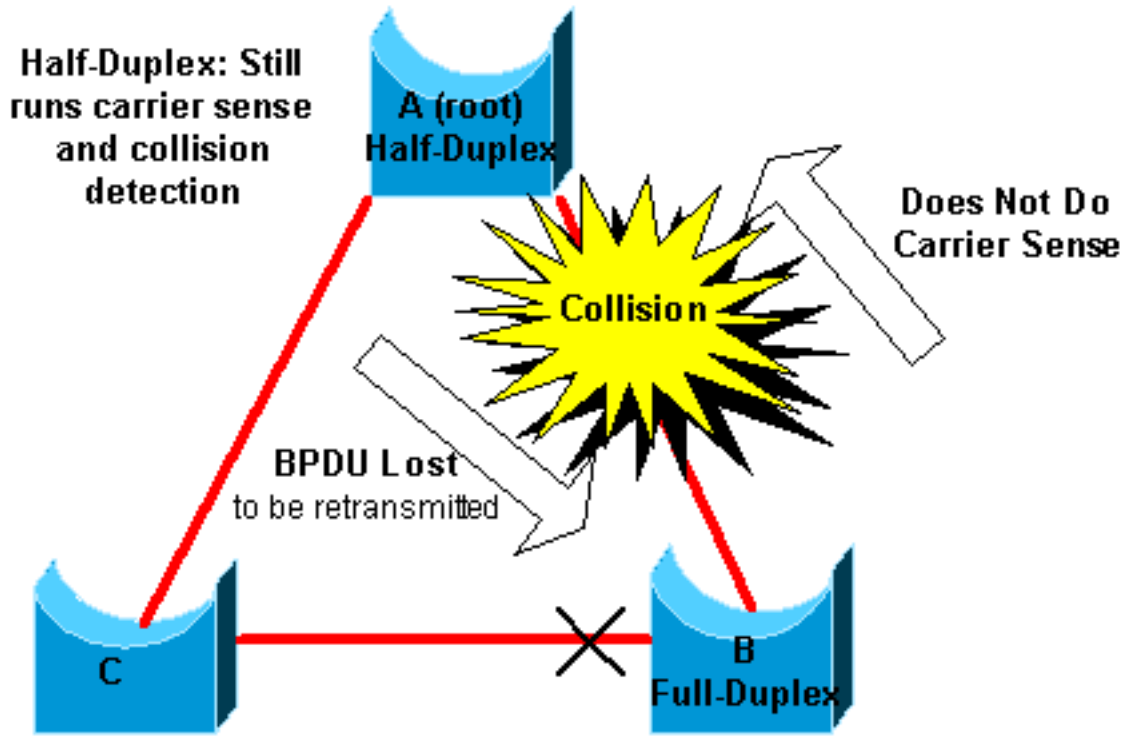
Convergenza dello Spanning Tree

Fare riferimento al video sullo Spanning Tree per vedere un esempio che spiega come inizialmente converge. L'esempio spiega anche perché una porta bloccata entra in modalità di inoltro a causa di un'eccessiva perdita di BPDU, con conseguente errore dell'STA.

Questo documento elenca inoltre le varie situazioni che possono causare errori dell'STA. La maggior parte di questi errori si riferisce a una perdita enorme di BPDU. La perdita causa il passaggio delle porte bloccate alla modalità di inoltro.

Mancata corrispondenza del duplex

La mancata corrispondenza duplex su un collegamento point-to-point è un errore di configurazione molto comune. Se si imposta manualmente la modalità duplex su Full su un lato del collegamento e si lascia l'altro lato in modalità di negoziazione automatica, il collegamento termina in half-duplex. (Una porta con modalità duplex impostata su Full non negozia più).



Lo scenario peggiore si ha quando un bridge che invia BPDU ha la modalità duplex impostata su half-duplex su una porta, ma la porta peer sull'altra estremità del collegamento ha la modalità

duplex impostata su full-duplex. Nell'esempio precedente, la mancata corrispondenza del duplex sul collegamento tra il ponte A e il ponte B può facilmente portare a un loop di bridging. Poiché il bridge B ha una configurazione full-duplex, non esegue il rilevamento del vettore prima dell'accesso al collegamento. Il ponte B inizia a inviare fotogrammi anche se il ponte A utilizza già il collegamento. Questa situazione è un problema per A; il ponte A rileva una collisione ed esegue l'algoritmo backoff prima che il ponte tenti un'altra trasmissione del frame. Se il traffico da B a A è sufficiente, ogni pacchetto inviato da A, incluse le BPDU, subisce differimento o collisione e alla fine viene eliminato. In termini di STP, poiché il bridge B non riceve più BPDU da A, il bridge B ha perso il bridge root. Questa situazione porta B a sbloccare la porta collegata al bridge C, creando il loop.

Ogniqualvolta si verifica una mancata corrispondenza duplex, questi messaggi di errore si trovano sulle console dei Catalyst switch che eseguono CatOS e il software Cisco IOS:

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

Software Cisco IOS

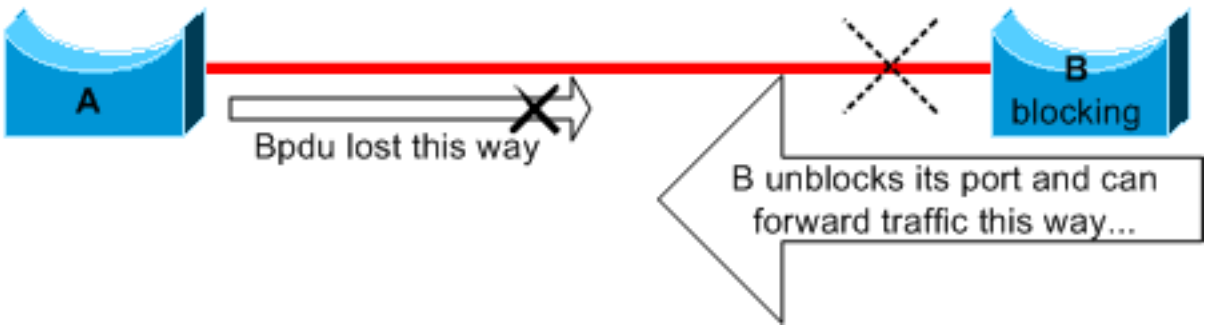
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

Controllare le impostazioni duplex e, se la configurazione duplex non corrisponde, impostarla in modo appropriato.

Per ulteriori informazioni sulla risoluzione dei problemi di mancata corrispondenza duplex, consultare il documento Configurazione e risoluzione dei problemi di negoziazione automatica Half/Full Duplex su Ethernet da 10/10/1000 Mb .

Collegamento unidirezionale

I collegamenti unidirezionali sono una causa comune di bridging loop. Sui collegamenti in fibra ottica, un errore senza rilevamento spesso causa collegamenti unidirezionali. Un'altra causa può essere un problema con un ricetrasmettitore. Tutto ciò che può portare un collegamento a restare in piedi e fornire una comunicazione unidirezionale è molto pericoloso in termini di STP. Ecco un esempio per chiarire:



Qui, supponiamo che il collegamento tra A e B sia unidirezionale. Il collegamento rimuove il traffico da A a B mentre trasmette il traffico da B ad A. Si supponga che il bridge B fosse in stato di blocco prima che il collegamento diventasse unidirezionale. Tuttavia, una porta può bloccare solo

se riceve BPDU da un bridge con una priorità più alta. Poiché, in questo caso, tutte le BPDU provenienti da A sono perse, il bridge B alla fine fa passare la sua porta verso A allo stato di inoltro e inoltra il traffico. Questo si ripete ciclicamente. Se questo errore si verifica all'avvio, il protocollo STP non converge correttamente. In caso di mancata corrispondenza del duplex, il riavvio aiuta temporaneamente; in questo caso, tuttavia, il riavvio dei bridge non ha assolutamente alcun effetto.

Per rilevare i collegamenti unidirezionali prima della creazione del loop di inoltro, Cisco ha progettato e implementato il protocollo UDLD (UniDirectional Link Detection). Questa funzione può rilevare cavi o collegamenti unidirezionali errati sul layer 2 e interrompere automaticamente i loop risultanti disabilitando alcune porte. Eseguire l'UDLD ove possibile in un ambiente con bridge.

Per ulteriori informazioni sull'uso dell'UDLD, fare riferimento al documento Descrizione e configurazione del protocollo UDLD (UniDirectional Link Detection).

Danneggiamento del pacchetto

Il danneggiamento del pacchetto può determinare lo stesso tipo di errore. Se un collegamento presenta un alto tasso di errori fisici, è possibile perdere un certo numero di BPDU consecutive. Tale perdita può far sì che una porta di blocco passi allo stato di inoltro. Questo caso non è molto frequente perché i parametri STP predefiniti sono molto conservativi. La porta di blocco deve perdere BPDU per 50 secondi prima di passare allo stato di inoltro. La trasmissione di una singola BPDU interrompe il ciclo. Questa situazione si verifica in genere in caso di regolazione non accurata dei parametri STP. Un esempio di regolazione è la riduzione max-age.

La mancata corrispondenza del duplex, cavi danneggiati o di lunghezza inadatta possono danneggiare i pacchetti. Per informazioni sull'output del contatore di errori di CatOS e del software Cisco IOS, consultare il documento Risoluzione dei problemi di porta e interfaccia degli switch.

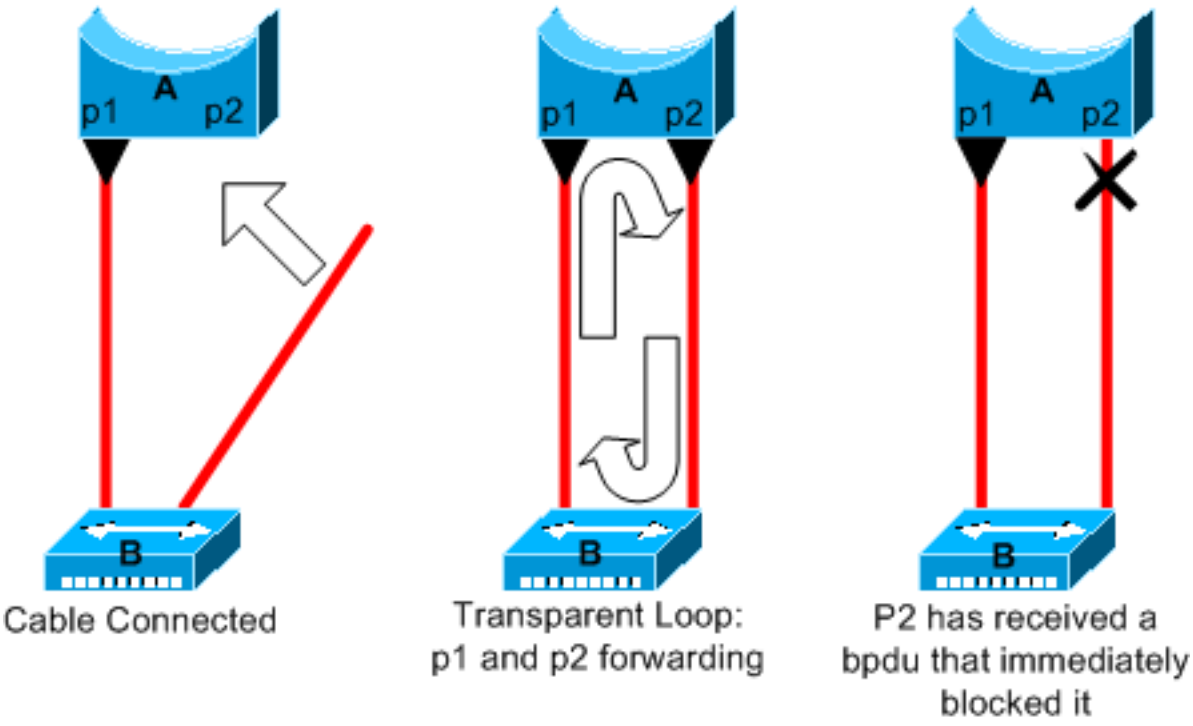
Errori delle risorse

L'STP è implementato nel software, anche su switch di fascia alta che svolgono la maggior parte delle funzioni di switching in hardware con ASIC (Specialized Application-Specific Integrated Circuit). Se per qualsiasi motivo si verifica un utilizzo eccessivo della CPU del bridge, le risorse possono essere inadeguate per la trasmissione di BPDU. L'STA generalmente non è ad alta intensità di processore e ha priorità su altri processi. La sezione Ricerca di errori delle risorse di questo documento fornisce alcune linee guida sul numero di istanze STP che una particolare piattaforma può gestire.

Errore di configurazione PortFast

PortFast è una funzionalità solitamente abilitata solo per una porta o un'interfaccia che si connette a un host. Quando il collegamento arriva su questa porta, il bridge salta le prime fasi dell'STA e passa direttamente alla modalità di inoltro.

> **Attenzione**: non usare la funzione PortFast sulle porte o sulle interfacce dello switch che si connettono ad altri switch, hub o router. In caso contrario, è possibile creare un loop di rete.



In questo esempio, il dispositivo A è un bridge con la porta p1 in fase di inoltro. La porta p2 ha una configurazione PortFast. Il dispositivo B è un hub. Non appena si collega il secondo cavo alla porta A, la porta p2 passa alla modalità di inoltro e crea un loop tra p1 e p2. Questo loop si arresta non appena p1 o p2 riceve una BPDU che mette una di queste due porte in modalità di blocco. Tuttavia questo tipo di ciclo transitorio è problematico. Se il traffico in loop è molto intenso, il bridge può avere problemi a trasmettere correttamente la BPDU che arresta il loop. Questo può ritardare notevolmente la convergenza o, in casi estremi, far crollare la rete.

Per ulteriori informazioni sull'uso corretto di PortFast sugli switch che eseguono CatOS e il software Cisco IOS, consultare il documento Utilizzo di PortFast e altri comandi per correggere i ritardi di connettività all'avvio della postazione di lavoro.

Con la configurazione PortFast, la porta o l'interfaccia partecipa all'STP. Se uno switch con una priorità di bridge inferiore a quella del root bridge attivo si collega a una porta o un'interfaccia configurata con PortFast, può essere scelto come bridge di root. Questa modifica del root bridge può influire negativamente sulla topologia dell'STP attivo e rendere la rete non ottimale. Per evitare questa situazione, la maggior parte dei Catalyst switch che eseguono CatOS e il software Cisco IOS ha una funzione nota come BPDU Guard. BPDU Guard disabilita una porta o un'interfaccia configurata con PortFast se la porta o l'interfaccia riceve una BPDU.

Per ulteriori informazioni sull'uso della funzione BPDU Guard sugli switch che eseguono CatOS e il software Cisco IOS, fare riferimento al documento Miglioramento di Spanning Tree Portfast con BPDU Guard.

Problemi di regolazione dei parametri STP e di diametro

Un valore aggressivo del parametro max-age e il ritardo di trasmissione possono determinare una topologia STP molto instabile. In questi casi, la perdita di alcune BPDU può determinare un loop. Un altro problema poco noto riguarda il diametro della rete di bridge. I valori predefiniti conservativi per i timer STP impongono un diametro di rete massimo di sette. Questo diametro massimo della rete limita la distanza tra i bridge della rete. In questo caso, due bridge distinti non possono essere distanti più di sette hop l'uno dall'altro. Parte di questa limitazione deriva dal campo age delle BPDU.

Quando una BPDU si propaga dal bridge root verso le ramificazioni della struttura ad albero, il campo age aumenta ogni volta che la BPDU passa attraverso un bridge. Quando il campo age supera il limite massimo, il bridge elimina la BPDU. Se il root è troppo lontano da alcuni bridge di rete, può verificarsi questo problema. Questo problema riguarda la convergenza dello spanning tree.

Prestare particolare attenzione se si prevede di modificare i timer STP rispetto al valore predefinito. Se si tenta di ottenere una riconvergenza più rapida in questo modo, può risultare pericoloso. Una modifica del timer STP influisce sul diametro della rete e sulla stabilità dell'STP. È possibile modificare la priorità del bridge per selezionare il root bridge e modificare il costo della porta o il parametro di priorità per controllare la ridondanza e il bilanciamento del carico.

Il software Cisco Catalyst offre macro che consentono di ottimizzare i principali parametri STP:

- OSPF (Open Shortest Path First) **set spantree root [secondary]** Il comando macro riduce la priorità del bridge in modo che diventi il bridge principale (o una radice alternativa). Per questo comando è disponibile un'opzione aggiuntiva che consente di ottimizzare i timer STP specificando il diametro della rete. Anche se eseguita correttamente, la regolazione del timer non migliora in modo significativo il tempo di convergenza e introduce alcuni rischi di instabilità della rete. Inoltre, questo tipo di ottimizzazione deve essere aggiornata ogniqualvolta un dispositivo viene aggiunto alla rete. Mantenere i valori predefiniti conservativi, che sono familiari ai tecnici di rete.
- OSPF (Open Shortest Path First) **set spantree uplinkfast** per CatOS o **spanning-tree uplinkfast** per il software Cisco IOS aumenta la priorità dello switch in modo che lo switch non possa essere root. Il comando aumenta il tempo di convergenza STP in caso di errore di uplink. Utilizzare questo comando su uno switch di distribuzione con connessione doppia ad alcuni switch core. Fare riferimento al documento Descrizione e configurazione della funzionalità Cisco UplinkFast.
- OSPF (Open Shortest Path First) **set spantree backbonefast enable** per CatOS o **spanning-tree backbonefast** del software Cisco IOS può aumentare il tempo di convergenza STP dello switch in caso di errore indiretto del collegamento. BackboneFast è una funzionalità proprietaria di Cisco. Fare riferimento al documento Descrizione e configurazione della funzionalità Backbone Fast sui Catalyst switch.

Per ulteriori informazioni sui timer STP e sulle regole per ottimizzarli quando necessario, fare riferimento al documento Descrizione e ottimizzazione dei timer del protocollo Spanning Tree.

Errori del software

Come indicato nell'Introduzione, l'STP è una delle prime funzionalità implementate nei prodotti Cisco. Questa funzionalità è molto stabile. Solo l'interazione con le funzionalità più recenti, come EtherChannel, ha causato errori STP in alcuni casi molto specifici che sono stati risolti. Fattori diversi possono causare un bug del software e avere diversi effetti. Non è possibile descrivere adeguatamente i problemi che un bug può causare. La situazione più pericolosa che può verificarsi a causa di errori software è se si ignorano alcune BPDU o se si ha una transizione della porta di blocco verso l'inoltro.

Risoluzione di un errore

Purtroppo, non esiste una procedura sistematica per risolvere un problema STP. Tuttavia, questa

sezione riassume alcune delle azioni disponibili. La maggior parte dei passaggi di questa sezione riguarda la risoluzione dei problemi dei bridging loop in generale. È possibile utilizzare un approccio più tradizionale per identificare altri errori dell'STP che comportano una perdita di connettività. Ad esempio, è possibile esplorare il percorso seguito dal traffico su cui si verifica un problema.

> **Nota**: la maggior parte di questi passaggi per la risoluzione dei problemi presuppone una connettività ai diversi dispositivi della rete bridge. Questa connettività indica l'accesso alla console. Durante un bridging loop, ad esempio, probabilmente non è possibile stabilire una connessione Telnet.

Se si dispone dell'output di un **show-tech support** dal dispositivo Cisco, è possibile usare Cisco CLI Analyzer (solo utenti registrati) per visualizzare i potenziali errori e correggerli.

Uso del diagramma della rete

Prima di risolvere un bridging loop, è necessario conoscere almeno questi elementi:

- Topologia della rete bridge
- Posizione del bridge root
- Posizione delle porte bloccate e dei collegamenti ridondanti

Queste informazioni sono essenziali per almeno questi due motivi:

- Per sapere che cosa risolvere in una rete, è necessario sapere com'è la rete quando funziona correttamente.
- La maggior parte delle procedure per la risoluzione dei problemi si basa sull'utilizzo **show** comandi per cercare di identificare le condizioni di errore. La conoscenza della rete consente di concentrarsi sulle porte critiche dei principali dispositivi.

Identificazione di un bridging loop

In passato, una tempesta di trasmissione poteva avere un effetto disastroso sulla rete. Oggi, con i collegamenti ad alta velocità e i dispositivi che forniscono lo switching a livello di hardware, è improbabile che un singolo host, ad esempio un server, interrompa una rete durante le trasmissioni. Il modo migliore per identificare un bridging loop è acquisire il traffico su un collegamento saturo e controllare che vengano visualizzati più volte pacchetti simili. Realisticamente, tuttavia, se tutti gli utenti in un determinato dominio di bridge hanno problemi di connettività allo stesso tempo, si può già sospettare un bridging loop.

Controllare l'utilizzo della porta sui dispositivi e cercare valori anomali. Fare riferimento alla sezione Controlla utilizzo porta di questo documento.

Sugli switch Catalyst con software CatOS, è possibile controllare facilmente l'utilizzo complessivo del backplane con **show system** Il comando fornisce l'utilizzo corrente del backplane dello switch e specifica anche l'utilizzo di picco e la data di utilizzo di picco. Un picco di utilizzo insolito mostra se c'è mai stato un bridging loop su questo dispositivo.

Rapido ripristino della connettività e riallestimento

Disabilitazione delle porte per interrompere il loop

Il bridging loop ha conseguenze estremamente gravi su una rete bridge. In genere, gli amministratori non hanno il tempo di cercare la causa del loop e preferiscono ripristinare la connettività il prima possibile. In questo caso, la soluzione più semplice è disabilitare manualmente tutte le porte che forniscono ridondanza nella rete. Se è possibile identificare una parte della rete più colpita, iniziare a disabilitare le porte in quell'area. Oppure, se possibile, disattivare inizialmente le porte che possono essere bloccate. Ogni volta che si disattiva una porta, verificare se è stata ripristinata la connettività nella rete. Identificando la porta disabilitata che arresta il loop, è possibile identificare anche il percorso ridondante in cui si trova la porta. Se la porta è stata bloccata, probabilmente è stato trovato il collegamento in cui si è verificato l'errore.

Registrazione di eventi STP su dispositivi che ospitano porte bloccate

Se non è possibile identificare con precisione l'origine del problema o se il problema è transitorio, abilitare la registrazione degli eventi STP sui bridge e sugli switch della rete su cui si verifica l'errore. Se si desidera limitare il numero di dispositivi da configurare, abilitare almeno questa funzionalità di accesso ai dispositivi che ospitano porte bloccate. La transizione di una porta bloccata è ciò che crea un loop.

- Software Cisco IOS-Eseguire il comando exec **debug spanning-tree events** per abilitare le informazioni di debug STP. Eseguire il comando general config mode **logging buffered** per acquisire le informazioni di debug nei buffer dei dispositivi.
- CatOS-The **set logging level spantree 7 default** aumenta il livello predefinito degli eventi correlati a STP al livello di debug. Accertarsi di aver registrato il numero massimo di messaggi nei buffer dello switch utilizzando **set logging buffer 500**

Èinoltre possibile provare a inviare l'output di debug a un dispositivo syslog. Purtroppo, quando si verifica un bridging loop, raramente si mantiene la connettività a un server syslog.

Controllo delle porte

Le porte critiche da analizzare per prime sono le porte di blocco. In questa sezione viene fornito un elenco degli elementi da cercare sulle diverse porte, con una breve descrizione dei comandi da impartire per gli switch che eseguono CatOS e il software Cisco IOS.

Verificare che le porte bloccate ricevano le BPDU

Soprattutto sulle porte bloccate e root, verificare periodicamente di ricevere le BPDU. Vari problemi possono determinare errori di ricezione di pacchetti o BPDU nelle porte.

- Software Cisco IOS-In Software Cisco IOS versione 12.0 o successive, output del **show spanning-tree bridge-group #** ha un campo `BPDU`. Il campo mostra il numero di BPDU ricevute per ogni interfaccia. Utilizzare il comando una o due volte in più per determinare se il dispositivo riceve le BPDU.Se il campo `BPDU` non è presente nell'output di **show spanning-tree** , è possibile abilitare il debug STP con il comando **debug spanning-tree** per verificare la ricezione di BPDU.
- CatOS-The **show mac module/port** indica il numero di pacchetti multicast ricevuti da una porta specifica. Ma il comando più semplice da utilizzare è **show spantree statistics module#/port# vlan#** Questo comando visualizza il numero esatto di BPDU di configurazione ricevute da una porta specifica, su una VLAN specifica. Una porta può appartenere a più VLAN, se abilitata per il

trunking. Vedere la sezione Comando aggiuntivo CatOS di questo documento.

Verificare l'eventuale mancata corrispondenza duplex

Per cercare una mancata corrispondenza duplex, è necessario controllare ogni lato del collegamento point-to-point.

- Software Cisco IOS-Emettere il comando **show interfaces [interface interface-number] status** per controllare la velocità e lo stato duplex della porta specifica.
- CatOS-Le prime righe dell'output del **show port module#/port#** Questa opzione permette di ottenere la velocità e la modalità duplex in base alla configurazione della porta.

Controllare l'utilizzo delle porte

Un'interfaccia con sovraccarico di traffico può non riuscire a trasmettere le BPDU vitali. Un sovraccarico del collegamento indica anche un possibile bridging loop.

- Software Cisco IOS-Usare il comando **show interfaces** per determinare l'utilizzo su un'interfaccia. In questo campo sono disponibili diversi campi, ad esempio `load` (carico) e `packets input/output` (ingresso/uscita pacchetti). Per una spiegazione dei problemi relativi alle porte e alle interfacce dello switch, consultare il documento sulla risoluzione dei problemi **show interfaces** output del comando.
- CatOS-The **show mac module#/port#** Questo comando visualizza le statistiche sui pacchetti ricevuti e inviati da una porta. OSPF (Open Shortest Path First) **show top** valuta automaticamente l'utilizzo della porta su un periodo di 30 secondi e visualizza il risultato. Il comando classifica i risultati in base all'utilizzo percentuale della larghezza di banda, anche se sono disponibili altre opzioni di classificazione. Inoltre, la **show system** fornisce un'indicazione dell'utilizzo del backplane, anche se il comando non punta a una porta specifica.

Verifica del danneggiamento dei pacchetti

- Software Cisco IOS-Cercare gli incrementi di errore nel contatore `degli errori di input` del **show interfaces** I contatori di errori sono runts, giant, no buffer, CRC, frame, overrun e ignored counts.Per una spiegazione dei problemi relativi alle porte e alle interfacce dello switch, consultare il documento sulla risoluzione dei problemi **show interfaces** command output.
- CatOS-The, comando **show port module#/port#** In vengono forniti alcuni dettagli con i campi `Align-Err, FCS-Err, Xmit-Err, Rcv-Err` e `Undersize`. OSPF (Open Shortest Path First) **show counters module#/port#** fornisce statistiche ancora più dettagliate.

Comando CatOS aggiuntivo

Il comando **show spantree statistics module#/port# vlan#** fornisce informazioni molto precise su una porta specifica. Utilizzare questo comando sulle porte sospette e prestare particolare attenzione ai seguenti campi:

- `Conteggio transazioni in avanti`: questo contatore indica quante volte una porta passa dall'apprendimento all'inoltro. In una topologia stabile, questo contatore indica sempre 1. Il contatore viene reimpostato su 0 quando la porta si abbassa e si solleva. Quindi, un valore

maggiore di 1 indica che la transizione sperimentata dalla porta è il risultato di un ricalcolo STP. La transizione non è il risultato di un errore di collegamento diretto.

- `Conteggio scadenze età max` - Questo contatore consente di tenere traccia del numero di volte in cui la validità massima è scaduta per questo collegamento. Fondamentalmente, una porta che prevede che le BPDU attendano il tempo massimo prima di considerare il bridge designato come perso. Il valore max age predefinito è 20 secondi. Ogni volta che si verifica questo evento, il contatore aumenta. Quando il valore non è 0, il bridge designato per questa LAN è instabile o presenta un problema con la trasmissione di BPDU.

Ricerca di errori delle risorse

Un utilizzo elevato della CPU può essere pericoloso per un sistema che esegue lo STA. Utilizzare questo metodo per verificare che la risorsa CPU di un dispositivo sia adeguata:

- Software Cisco IOS: immettere il comando **show processes cpu.** Verificare che l'utilizzo della CPU non sia troppo elevato. Per i Catalyst switch serie 4500/4000 che eseguono CatOS o il software Cisco IOS, consultare il documento Utilizzo della CPU sui Catalyst switch 4500/4000, 2948G, 2980G e 4912G.
- CatOS-Invio del comando **show proc cpu** command to display CPU utilization information. Check that the CPU utilization is not too high.

Esiste una limitazione al numero di diverse istanze di STP che un Supervisor Engine può gestire. Assicurarsi che il numero totale di porte logiche in tutte le istanze di STP per VLAN diverse non superi il numero massimo supportato per ogni tipo di motore Supervisor e configurazione di memoria.

Utilizzare il comando **show spantree summary** per gli switch con CatOS o **show spanning-tree summary totals** per switch con software Cisco IOS. Questi comandi visualizzano il numero di porte logiche o interfacce per ciascuna VLAN nella colonna `STP Active`. Il totale viene visualizzato nella parte inferiore di questa colonna. Il totale rappresenta la somma di tutte le porte logiche su tutte le istanze di STP per le diverse VLAN. Accertarsi che questo numero non superi il numero massimo supportato per ciascun tipo di Supervisor Engine.

Nota: la formula per calcolare la somma delle porte logiche sullo switch è:

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

Per un riepilogo delle limitazioni STP che si applicano ai Catalyst switch, fare riferimento a questi documenti:

Piattaforma	Limitazioni STP di CatOS	Limitazioni STP del software Cisco IOS
Catalyst 6500/6000 Supervisor Engine I e II	Risoluzione dei problemi STP	
Catalyst 6500/6000 Supervisor Engine 720	Risoluzione dei problemi STP	Risoluzione dei problemi Spanning Tree
Catalyst 4500/4000	Spanning Tree	Spanning Tree risoluzione dei problemi
Catalyst 3750		Configurazione STP

Disabilitazione delle funzioni non necessarie

Quando si esegue la risoluzione dei problemi, si cerca di identificare il problema corrente nella rete. Disabilitare il maggior numero possibile di funzioni. La disabilitazione aiuta a semplificare la struttura della rete e facilita l'identificazione del problema. Ad esempio, EtherChanneling è una funzione che richiede l'uso del protocollo STP per combinare logicamente diversi collegamenti in un singolo collegamento; è consigliabile disabilitare questa funzione durante il processo di risoluzione dei problemi. In generale, per semplificare al massimo la configurazione, è consigliabile semplificare notevolmente la procedura di risoluzione dei problemi.

Comandi utili

Comandi Cisco IOS Software

- **show interfaces**
- **show spanning-tree**
- **show bridge**
- **show processes cpu**
- **debug spanning-tree**
- **logging buffered**

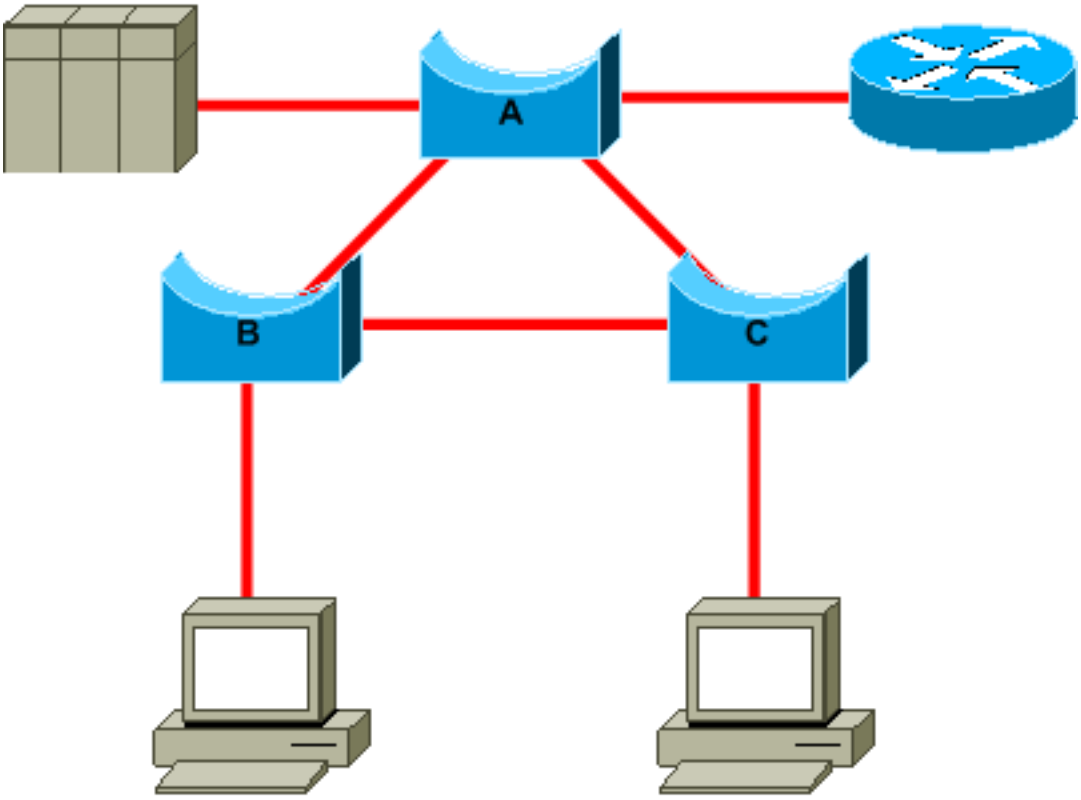
Comandi CatOS

- **show port**
- **show mac**
- **show spantree**
- **show spantree statistics**
- **show spantree blockedports**
- **show spantree summary**
- **show top**
- **show proc cpu**
- **show system**
- **show counters**
- **set spantree root [secondary]**
- **set spantree uplinkfast**
- **set logging level**
- **set logging buffered**

Design dell'STP per evitare problemi

Identificazione della posizione del root

Molto spesso, le informazioni sulla posizione di root non sono disponibili al momento della risoluzione dei problemi. Non lasciare l'STP per identificare il bridge root. Per ogni VLAN, in genere è possibile identificare quale switch può servire come root. Questo dipende dal design della rete. In genere, scegliere un bridge potente in mezzo alla rete. Se si posiziona il bridge root al centro della rete con connessione diretta ai server e ai router, in genere si riduce la distanza media dai client ai server e ai router.



Questo diagramma mostra:

- Se B è il bridge root, il link da A a C è bloccato sul bridge A o sul bridge C. In questo caso, gli host che si connettono allo switch B possono accedere al server e al router in due hop. Gli host che si connettono al bridge C possono accedere al server e al router in tre hop. La distanza media è di due hop e mezzo.
- Se A è il bridge root, il router e il server sono raggiungibili in due hop per entrambi gli host che si connettono su B e C. La distanza media in questo caso è di due hop.

La logica alla base di questo semplice esempio viene trasferita a topologie più complesse.

> **Nota**: per ciascuna VLAN, configurare il bridge radice e il bridge radice di backup riducendo il valore del parametro di priorità STP. In alternativa, è possibile utilizzare la macro set spantree root .

Identificazione della ridondanza

Pianificare l'organizzazione dei collegamenti ridondanti. Dimenticare la funzionalità plug-and-play dell'STP. Regolare il parametro di costo dell'STP per decidere quali porte bloccare. Questa ottimizzazione di solito non è necessaria se si dispone di un design gerarchico e di un bridge root in una buona posizione.

> **Nota**: per ciascuna VLAN, individuare le porte che possono essere bloccate nella rete stabile. Disporre di un diagramma di rete che mostra chiaramente ogni loop fisico nella rete che le porte bloccate interrompono i loop.

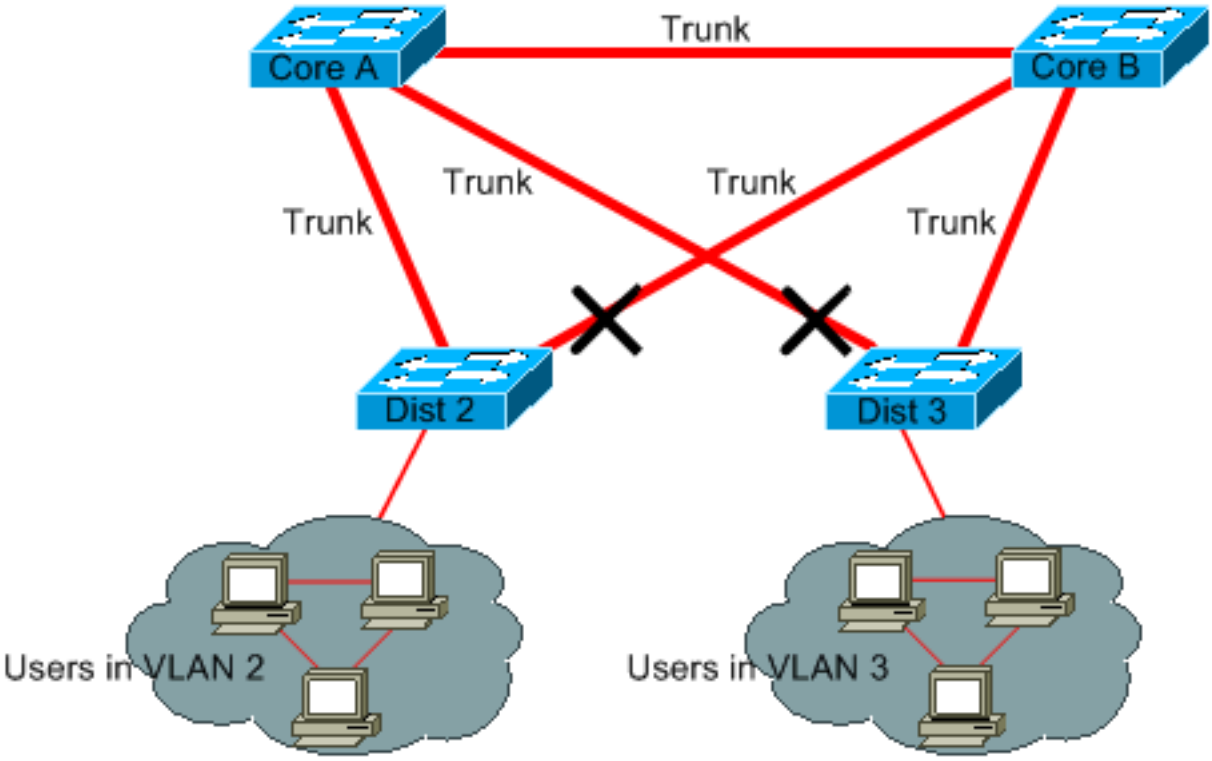
Conoscere la posizione dei collegamenti ridondanti consente di identificare un bridging loop accidentale e la relativa causa. Inoltre, conoscere la posizione delle porte bloccate consente di capire dove sta l'errore.

Riduzione al minimo del numero di porte bloccate

L'unica azione critica che l'STP esegue è il blocco delle porte. Una singola porta di blocco che passa erroneamente all'inoltro può fondere gran parte della rete. Un buon modo per limitare il rischio insito nell'uso dell'STP consiste nel ridurre il più possibile il numero di porte bloccate.

Eliminazione delle VLAN non utilizzate

Non sono necessari più di due collegamenti ridondanti tra due nodi in una rete bridge. Tuttavia, è comune questo tipo di configurazione:

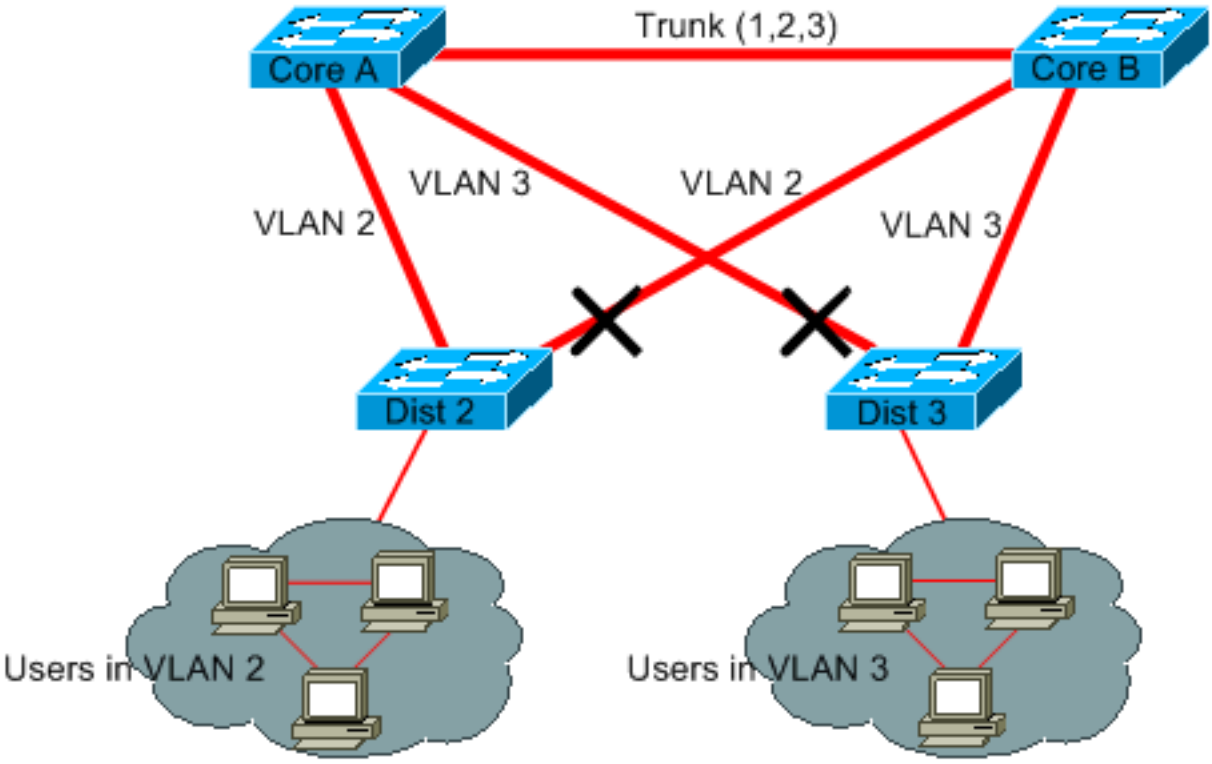


Gli switch di distribuzione sono collegati due volte a due core switch. Gli utenti che si connettono agli switch di distribuzione appartengono solo a un sottoinsieme delle VLAN disponibili nella rete. Nell'esempio, gli utenti che si connettono al Dist 2 sono tutti sulla VLAN 2; il Dist 3 connette gli utenti solo sulla VLAN 3. Per impostazione predefinita, i trunk trasportano tutte le VLAN definite nel dominio VLAN Trunk Protocol (VTP). Solo la directory 2 riceve traffico broadcast e multicast non necessario per la VLAN 3, ma sta anche bloccando una delle sue porte per la VLAN 3. Il risultato sono tre percorsi ridondanti tra il core A e il core B. Questa ridondanza determina un numero maggiore di porte bloccate e una maggiore probabilità di loop.

> **Nota**: eliminare le VLAN non necessarie dai trunk.

L'eliminazione del VTP può essere utile, ma questo tipo di funzionalità plug-and-play non è necessaria nel core della rete.

In questo esempio, viene utilizzata solo una VLAN di accesso per collegare gli switch di distribuzione al core:



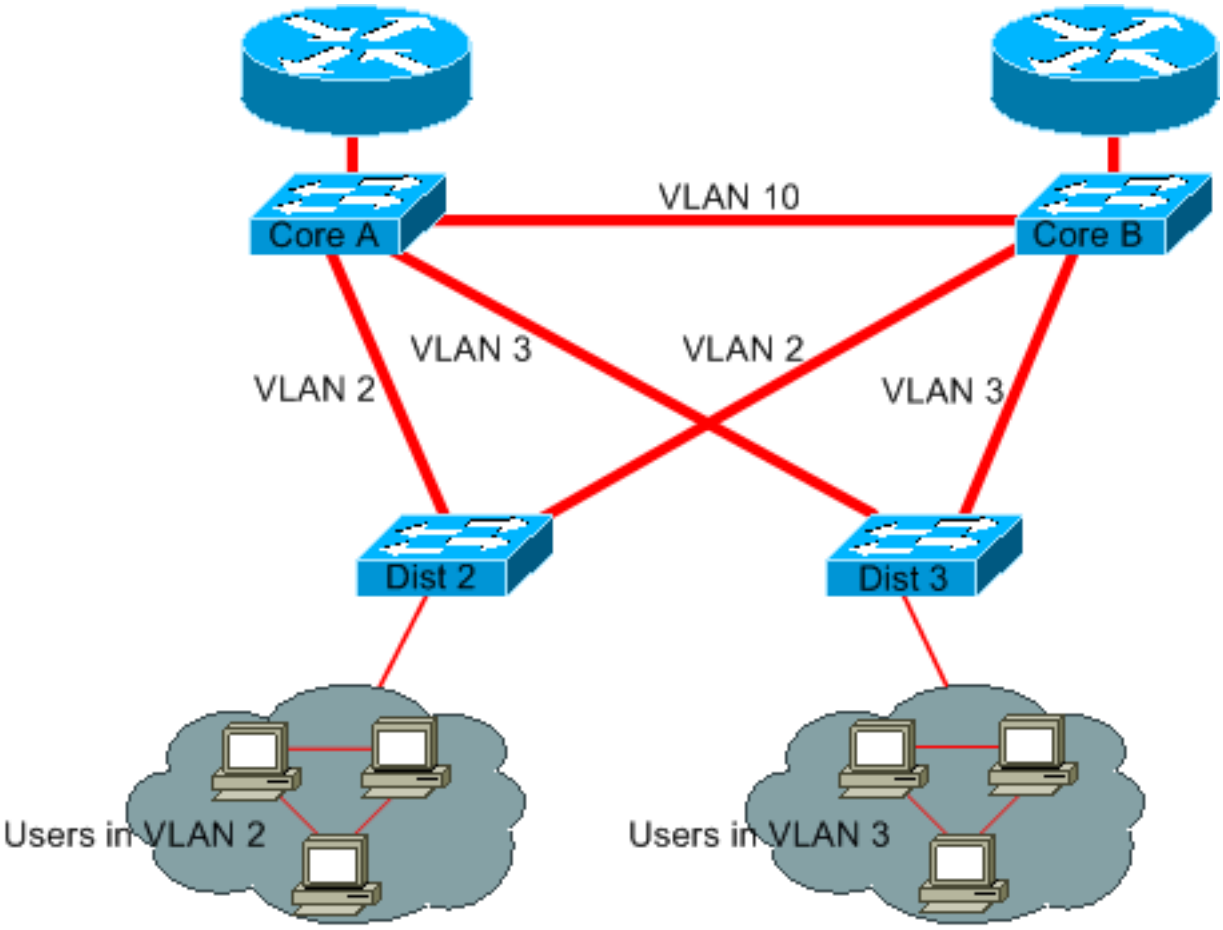
In questo design, viene bloccata una sola porta per ciascuna VLAN. Inoltre, con questo design, è possibile rimuovere tutti i collegamenti ridondanti in un solo passaggio se si arresta il Core A o il Core B.

Utilizzo dello switching di livello 3

Utilizzare lo switching di livello 3 significa eseguire il routing approssimativamente alla velocità di switching. Un router svolge due funzioni principali:

- Un router crea una tabella di inoltro. Il router generalmente scambia informazioni con i colleghi tramite protocolli di routing.
- Un router riceve i pacchetti e li inoltra all'interfaccia corretta in base all'indirizzo di destinazione.

Gli switch Cisco di livello 3 di fascia alta sono ora in grado di eseguire questa seconda funzione, alla stessa velocità della funzione di switching di livello 2. Se si introduce un hop di routing e si crea un'ulteriore segmentazione della rete, non vi è alcuna penalità in termini di velocità. Questo diagramma si basa sull'esempio riportato nella sezione Eliminazione delle VLAN che non si utilizzano:



In questo caso il Core A e il Core B sono switch di livello 3. La VLAN 2 e la VLAN 3 non sono più collegate tra Core A e Core B, quindi non è possibile creare un loop STP.

- La ridondanza è ancora presente e si basa su protocolli di routing di livello 3. Il design garantisce una riconvergenza ancora più veloce della riconvergenza con STP.
- Non vi è più alcuna porta singola bloccata dall' STP. Pertanto, non esiste alcun potenziale per un bridging loop.
- Non vi è alcuna penale in termini di velocità, in quanto lasciare la VLAN con lo switch di layer 3 è veloce quanto il bridging all'interno della VLAN.

Questo design presenta un unico svantaggio. La migrazione a questo tipo di struttura implica generalmente una rielaborazione dello schema di indirizzamento.

Mantenimento dell'STP anche se non è necessario

Anche se la rimozione di tutte le porte bloccate dalla rete è riuscita e non vi è ridondanza fisica, non disabilitare l'STP. Il protocollo STP in genere non richiede un uso intensivo del processore. Nella maggior parte degli switch Cisco, la commutazione di pacchetto non coinvolge la CPU. Inoltre, le poche BPDU inviate su ogni collegamento non riducono in modo significativo la larghezza di banda disponibile. Tuttavia, una rete bridge senza STP può fondersi in una frazione di secondo se, ad esempio, un operatore commette un errore su un pannello patch. In generale, non vale la pena disabilitare l'STP in una rete bridge .

Mantenimento del traffico lontano dalla VLAN di amministrazione e presenza di più VLAN su tutta la rete

Uno switch Cisco in genere ha un singolo indirizzo IP che si collega a una VLAN, nota come

VLAN di amministrazione. In questa VLAN, lo switch si comporta come un host IP generico. In particolare, ogni pacchetto broadcast o multicast viene inoltrato alla CPU. Un'elevata velocità di trasmissione o traffico multicast sulla VLAN di amministrazione può influire negativamente sulla CPU e sulla capacità della CPU di elaborare le BPDU vitali. Pertanto, mantenere il traffico degli utenti al di fuori della VLAN di amministrazione.

Fino a poco tempo fa, non era possibile rimuovere la VLAN 1 da un trunk nelle implementazioni Cisco. La VLAN 1 in genere funge da VLAN di amministrazione, con tutti gli switch accessibili nella stessa subnet IP. Sebbene utile, questa configurazione può essere pericolosa perché un bridging loop sulla VLAN 1 influisce su tutti i trunk, il che può arrestare l'intera rete. Naturalmente, lo stesso problema esiste indipendentemente dalla VLAN in uso. Provare a segmentare i domini bridging utilizzando gli switch di livello 3 ad alta velocità.

A partire da CatOS versione 5.4 e dal software Cisco IOS versione 12.1 (11b) E, è possibile rimuovere la VLAN 1 dai trunk. La VLAN 1 esiste ancora, ma blocca il traffico, impedendo qualsiasi possibilità di loop.

Informazioni correlate

- Strumenti e risorse - Supporto tecnico e documentazione
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).